

IN THE CLAIMS

Please amend the claims as set out below:

1. (previously presented) A method for providing secure authentication, the method comprising:

a) sending basic authentication data from a first computer to a second computer, wherein the basic authentication data provides a certificate including a validity status date and a credential, the credential being for permitting a first type of transaction access by the first computer to an application provided by the second computer, wherein the basic authentication data has been certified by an accepted certifying authority, and the basic authentication data sent to the second computer includes a public key of the first computer;

b) generating an additional individual authentication data unit by the first computer, wherein the additional individual authentication data unit provides a self certificate including a validity status date and a credential, the self certificate credential being for permitting a second type of access by the first computer to an application provided by the second computer, and wherein the generating includes:

signing the individual authentication data unit by the first computer using a key associated with the public key;

and

c) sending the additional individual authentication data unit by the first computer to the second computer, so that the second computer can verify authenticity of the additional individual authentication data unit using the first computer's public key that was received from the first computer by the second computer with the basic authentication data.

2. (previously presented) The method as claimed in claim 1 wherein the second type of access includes an access for an application in which a digital credit card is used for a purchase.

3. (previously presented) The method as claimed in claim 1, wherein the authenticity of said additional individual authentication data is established by signature of said accepted certifying authority.

4. (previously presented) The method as claimed in claim 1 wherein the second type of access includes an access for an application in which an email message is securely transmitted.

5. (previously presented) The method as claimed in claim 1, wherein the authentication data includes an identity certificate, and the method includes:

generating a command from the first computer for the second computer to invalidate a previously presented identity certificate, wherein the previously presented identity certificate includes a validity status date and an identity credential;

generating by the first computer a new identity certificate having a validity status date and an identity credential; and

sending, from the first computer to the second computer, the new identity certificate to replace the invalidated identity certificate, wherein the command to invalidate and the new identity certificate are both received by the second computer during the certain communication session.

6-15. (canceled)